Using Endpoint Telemetry to Accelerate the Baseline

Keith W. McCammon
baseline

noun | baseline | 'bāsˌlīn/

a usually initial set of critical observations or data used for comparison or a control; a starting point
Identifying what’s **good** . . .

makes it easier to spot what’s **bad**.

Duh.
memory

survey tools

logs
upside
know how to baseline a system
ready access to tools

know how to baseline a system
need to baseline hundreds, thousands
downside
“Using endpoint telemetry to accelerate the baseline . . .”
point-in-time $\Rightarrow$ ongoing
static  living
endpoint \quad \rightarrow \quad enterprise
collection
4,300 processes/day

86,400 events
258 million processes/day

~5 billion events

(x60K)
collection

filtering

analysis
What can you afford to evaluate?

“criteria”
~70 thousand events (wat)
criteria + hash

simple! 😊

good for point products, applications
~35 thousand events (hrm)
criteria + hash

(some) obvious problems
pesky dual-use tools 😞
pesky system services 😞
criteria + hash + relationship

writer | parent | child
criteria + hash
+ relationship
+ process metadata

user ID | command line
~10 thousand events
scope
some endpoints
all the things!
just this once . . .

permanence
“forever”
rly forever
the promised land!
Keith W. McCammon

@kwm | @redcanaryco